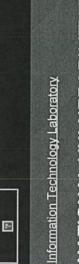
EXHIBIT 43

Case: 1:18-cv-00864 Document #: 897-14 Filed: 02/29/20 Page 2 of 7 PageID #:41603



NVD - Control - AC-2 - ACCOUNT MANAGEMENT





□ NVD MENU

800-53

(Rev. 4)

Moderate-Impact Other Links High-Impact Families

Security Controls _ow-Impact

Search

Security and Privacy Controls for Federal Information Systems and Organizations

NIST Special Publication 800-53 (Rev. 4)

REV4

800-53/800-53A

Jump To:

Supplemental Guidance Control Description

All Controls > AC > AC-2

Revision 4 Statements References

AC-2AC-2 (1) (2) (3) (4) AC-2 (1) (2) (3) (4) (5) (11) (12) (13)

Priority: P1 - Implement P1 security controls first.

Baseline Allocation: Low Moderate

Family: AC - ACCESS CONTROL

AC-2 ACCOUNT MANAGEMENT

Control Description

The organization:

- a. Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];
- b. Assigns account managers for information system accounts;
- c. Establishes conditions for group and role membership;
- d. Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
- e. Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

- NVD Control AC-2 ACCOUNT MANAGEMENT
- f. Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- g. Monitors the use of information system accounts;
- h. Notifies account managers:
- 1. When accounts are no longer required;
- 2. When users are terminated or transferred; and
- When individual information system usage or need-to-know changes;
- i. Authorizes access to the information system based on:
- 1. A valid access authorization;
- 2. Intended system usage; and
- 3. Other attributes as required by the organization or associated missions/business functions;
- j. Reviews accounts for compliance with account management requirements [Assignment: organization-defined requency]; and
- k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from

Supplemental Guidance

attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the information system availability. Temporary and emergency accounts are accounts intended for shortupgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of requiring administrative privileges on information system accounts receive additional scrutiny by Organizations may choose to define access privileges or other attributes by account, by type of example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account access privileges reflects the requirements in other security controls in the security plan. Users procedures when there is a need for short-term accounts without the demand for immediacy in account, or a combination of both. Other attributes required for authorizing access include, for term use. Organizations establish temporary accounts as a part of normal account activation remote access to support travel requirements). Failure to consider these factors could affect appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Information system account types include, for example, individual, shared, group, system,

normal account authorization processes. Emergency and temporary accounts are not to be confused not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts account activation. Organizations establish emergency accounts in response to crisis situations and organizations or when network resources are unavailable). Such accounts remain available and are required; or (ii) when individuals are transferred or terminated. Some types of information system with the need for rapid account activation. Therefore, emergency account activation may bypass include, for example: (i) when shared/group, emergency, or temporary accounts are no longer with infrequently used accounts (e.g., local logon accounts used for special tasks defined by accounts may require specialized training.

NVD - Control - AC-2 - ACCOUNT MANAGEMENT

Related to: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13

Control Enhancements

AC-2(1)	AC-2(1) ACCOUNT MANAGEMENT AUTOMATED SYSTEM ACCOUNT MANAGEMENT
	The organization employs automated mechanisms to support the management of information system accounts.
	Supplemental Guidance: The use of automated mechanisms can include, for example: using email or text messaging to automatically notify account
	managers when users are terminated or transferred; using the information system to monitor account usage; and using telephonic notification to report
	atypical system account usage.
AC-2(2)	AC-2(2) ACCOUNT MANAGEMENT REMOVAL OF TEMPORARY / EMERGENCY ACCOUNTS
	The information system automatically [Selection: removes; disables] temporary and emergency accounts after [Assignment: organization-
	defined time period for each type of account].

	Supplemental Guidance: This control enhancement requires the removal of both temporary and emergency accounts automatically after a predefined period of time has elapsed, rather than at the convenience of the systems administrator.
AC-2(3)	AC-2(3) ACCOUNT MANAGEMENT DISABLE INACTIVE ACCOUNTS
	The information system automatically disables inactive accounts after [Assignment: organization-defined time period].

	e		
	gnm		
	Assi		
	jes [
	notif		
	tions, and notifies [/		
	ns,		
	actic		
	oval		
	remo		
	and		
	ing,		
	sabli		
	g, di		
	plin		
	, ena		
	modification, enabling, disabling, and removal acti		
	lifica		
	mod		
	-		
	tior		
SNO	reation		
CTIONS	unt creatior		
IT ACTIONS	ccount creation, I		
AUDIT ACTIONS	lits account creation		
ED AUDIT ACTIONS	audits account creation	es].	
MATE	ally audits a	r roles].	
MATE	ically audits a	el or roles].	
MATE	ically audits a	sonnel or roles].	
MATE	ically audits a	personnel or roles].	
MATE	ically audits a	ined personnel or roles].	
MATE	ically audits a	defined personnel or roles].	
MATE	ically audits a	ation-defined personnel or roles].	
MATE	ically audits a	anization-defined personnel or roles].	
ACCOUNT MANAGEMENT AUTOMATE	ally audits a	organization-defined personnel or roles].	
MATE	ically audits a	organization-defined personnel or roles].	

Related to: AU-2, AU-12

AC-2(5)	AC-2(5) ACCOUNT MANAGEMENT INACTIVITY LOGOUT The organization requires that users log out when [Assignment: organization-defined time-period of expected inactivity or description of when to
	Related to: SC-23
AC-2(6)	ACCOUNT MANAGEMENT DYNAMIC PRIVILEGE MANAGEMENT The information system implements the following dynamic privilege management capabilities: [Assignment: organization-defined list of dynamic

NVD - Control - AC-2 - ACCOUNT MANAGEMENT

management can also refer to mechanisms that change the privileges of users based on dynamic rules as opposed to editing specific user profiles. This type mission/business requirements and operational needs of organizations. Dynamic privilege management can include, for example, the immediate revocation user privileges, dynamic access control approaches (e.g., service-oriented architectures) rely on run time access control decisions facilitated by dynamic of privilege management includes, for example, automatic adjustments of privileges if users are operating out of their normal work times, or if information Supplemental Guidance: In contrast to conventional access control approaches which employ static information system accounts and predefined sets of systems are under duress or in emergency maintenance situations. This control enhancement also includes the ancillary effects of privilege changes, for example, the potential changes to encryption keys used for communications. Dynamic privilege management can support requirements for information of privileges from users, as opposed to requiring that users terminate and restart their sessions to reflect any changes in privileges. Dynamic privilege privilege management. While user identities may remain relatively constant over time, user privileges may change more frequently based on ongoing

Related to: AC-16

ACCOUNT MANAGEMENT | ROLE-BASED SCHEMES AC-2(7)

The organization:

AC-2 (7)(a) Establishes and administers privileged user accounts in accordance with a role-based access scheme that organizes allowed information system access and privileges into roles;

AC-2 (7)(b) Monitors privileged role assignments; and

AC-2 (7)(c) Takes [Assignment: organization-defined actions] when privileged role assignments are no longer appropriate

relevant functions that ordinary users are not authorized to perform. These privileged roles include, for example, key management, account management, Supplemental Guidance; Privileged roles are organization-defined roles assigned to individuals that allow those individuals to perform certain securitynetwork and system administration, database administration, and web administration.

ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT CREATION AC-2(8)

The information system creates [Assignment: organization-defined information system accounts] dynamically.

Supplemental Guidance: Dynamic approaches for creating information system accounts (e.g., as implemented within service-oriented architectures) rely on establishing accounts (identities) at run time for entities that were previously unknown. Organizations plan for dynamic creation of information system accounts by establishing trust relationships and mechanisms with the appropriate authorities to validate related authorizations and privileges Related to: AC-16

ACCOUNT MANAGEMENT | RESTRICTIONS ON USE OF SHARED / GROUP ACCOUNTS AC-2(9)

The organization only permits the use of shared/group accounts that meet [Assignment: organization-defined conditions for establishing shared/group accounts].

ACCOUNT MANAGEMENT | SHARED / GROUP ACCOUNT CREDENTIAL TERMINATION AC-2(10)

The information system terminates shared/group account credentials when members leave the group.

ACCOUNT MANAGEMENT | USAGE CONDITIONS AC-2(11)

The information system enforces [Assignment: organization-defined circumstances and/or usage conditions] for [Assignment: organizationdefined information system accounts]. Supplemental Guidance: Organizations can describe the specific conditions or circumstances under which information system accounts can be used, for example, by restricting usage to certain days of the week, time of day, or specific durations of time.

ACCOUNT MANAGEMENT | ACCOUNT MONITORING / ATYPICAL USAGE AC-2(12)

The organization:

AC-2 (12)(a)

Monitors information system accounts for [Assignment: organization-defined atypical usage]; and

AC-2 (12)(b)

Reports atypical usage of information system accounts to [Assignment: organization-defined personnel or roles]

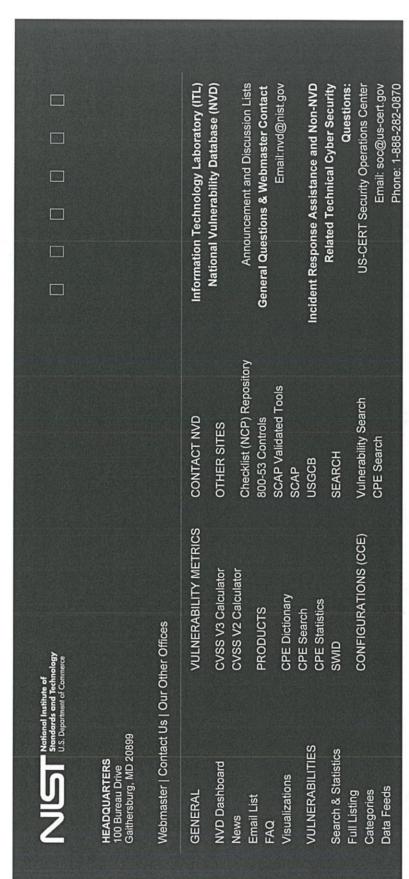
Supplemental Guidance: Atypical usage includes, for example, accessing information systems at certain times of the day and from locations that are not consistent with the normal usage patterns of individuals working in organizations. Related to: CA-7

ACCOUNT MANAGEMENT | DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS AC-2(13)

The organization disables accounts of users posing a significant risk within [Assignment: organization-defined time period] of discovery of the

impacts to organizational operations and assets, individuals, other organizations, or the Nation. Close coordination between authorizing officials, information Supplemental Guidance: Users posing a significant risk to organizations include individuals for whom reliable evidence or intelligence indicates either the intention to use authorized access to information systems to cause harm or through whom adversaries will cause harm. Harm includes potential adverse system administrators, and human resource managers is essential in order for timely execution of this control enhancement. Related to: PS-4

References



Privacy Statement | Privacy Policy | Security Notice | Accessibility Statement | NIST Privacy Program | No Fear Act Policy

Business USA | Healthcare.gov | Science.gov | USA.gov

Disclaimer | FOIA | Environmental Policy Statement | Cookie Disclaimer | Scientific Integrity Summary | NIST Information Quality Standards

Vendor Comments